论 文

基于布尔运算的 $(2, n)$ 秘密共享方案董琳^①, 王道顺^{①*}, 李顺东^②, 戴一奇^①^① 清华大学计算机科学与技术系, 北京 100084^② 陕西师范大学计算机科学学院, 西安 710062

* 通信作者. E-mail: daoshun@mail.tsinghua.edu.cn

收稿日期: 2009-07-17; 接受日期: 2010-07-01

国家自然科学基金 (批准号: 60873249, 60673065, 60902102, 60971006)、国家高技术研究发展计划 (批准号: 2008AA10Z419) 和

国家博士后基金 (批准号: 20090460316) 资助项目

摘要 基于多项式插值的秘密共享方案 (SS) 能精确重构秘密信息, 但其计算复杂度较高. 可视分存方案 (VSS) 利用人眼视觉效应重构秘密信息, 无需密码计算, 但存在像素膨胀和对照度的损失. Wang 等人提出了一种基于布尔运算的黑白图像 $(2, n)$ 秘密共享方案, 具有较低的计算复杂度, 无像素膨胀, 对照度为 $1/2$. 文中构造了黑白图像的 r 轮 $(2, n)$ 秘密共享方案, 提高了 Wang 等人方案的对照度; 采用两种不同的方法构造了灰度图像和彩色图像的 $(2, n)$ 秘密共享方案. 文中所构造的方案计算复杂度低, 重构密图的对照度高, 并且当 r 较大时, 接近精确重构.

关键词 秘密共享方案 布尔运算 半色调 对照度

1 引言

1979 年, Blakley^[1] 和 Shamir^[2] 各自独立的提出了秘密共享方案 (secret sharing, SS). 在 (k, n) 门限方案中, 秘密信息被分为 n 份 (称为分存) 分别交给 n 个参与者持有, 任何 k 个或更多参与者一起可利用其持有的分存重构出秘密信息, 而小于 k 个参与者则得不到任何秘密信息, 秘密共享方案提供了一种有效的保护秘密的方法. 之后, 一些研究者将 Shamir 的秘密共享方案进行扩展, 用于分存图像^[3–5]. 这类方案能精确重构秘密, 但由于其解密需要执行多项式插值, 因而计算复杂度较高, 尤其在处理图像时.

为了更好地分存图像, 降低重构的计算复杂度, Naor 和 Shamir^[6] 在 1994 年的欧密会上提出了可视分存方案 (visual secret sharing, VSS), 利用人眼视觉效应来恢复秘密信息, 无需进行复杂的密码计算. 这类方法将原始密图中的一个像素分存为分存图中的 m 个子像素, 因而存在像素膨胀和对照度的损失. 在文献 [7–10] 中, 一些研究者尝试了不同的方法, 减少像素膨胀, 提高对照度.

由此可见, 如何设计无像素膨胀, 同时又具有高对照度和低计算复杂度的秘密共享方案值得研究. Wang 等人^[11] 提出了两种秘密共享方案, 一种是灰度图像的 (n, n) 方案, 能精确重构密图; 一种是黑白图像的 $(2, n)$ 方案, 重构密图的对照度为 $1/2$. 这两种方案都是基于布尔运算构造的, 并且没有像素膨胀. 布尔运算计算复杂度低, 利用一般的图像处理软件, 如 Photoshop 等, 也可以很容易的实现布尔运算. Chao 和 Lin^[12] 通过一种带有冗余性的分发策略将 Wang 等的 (n, n) 方案扩展到一般的 (k, n)

引用格式: 董琳, 王道顺, 李顺东, 等. 基于布尔运算的 $(2, n)$ 秘密共享方案. 中国科学: 信息科学, 2011, 41: 513–525

方案. 基于 Wang 等人的 $(2, n)$ 方案, Chang 等人^[13] 通过选举策略和放弃最低有效位的方法, 构造了灰度图像的 $(2, n)$ 方案. Chang 等人^[14] 结合 Shamir 的方案和基于位图的搜索算法, 将 Wang 等人的 $(2, n)$ 方案扩展到彩色图像, 然而这种方法增加了计算复杂度. 因此, 如何提高 $(2, n)$ 方案重构密图的对照度, 设计有效的灰度和彩色分存方案值得研究.

本文首先构造了二值图像的 r 轮 $(2, n)$ 秘密共享方案, 将 Wang 等人方案的对照度由 $1/2$ 提高到 $\alpha^{(r)} = 1 - (1/2)^r$, 其中 $r \geq 1$. 然后给出了两种方法, 构造灰度图像的秘密共享方案, 一种方法是基于半色调技术, 另一种方法是基于比特位处理. 所提出的灰度图像秘密共享方案可以很容易地扩展到彩色图像. 与已有方案相比, 本文所构造的方案具有高对照度和低复杂度, 付出的代价是每个参与者需要持有多个分存图.

2 预备知识

2.1 Wang 等人的 $(2, n)$ 秘密共享方案

Wang 等人^[11] 提出了一个针对黑白二值图像的概率 $(2, n)$ -SS 方案, 该方案使用了布尔异或运算 (XOR, 记作 “ $\oplus$ ”) 和与运算 (AND, 记作 “ $\wedge$ ”), 生成 $n+1$ 个不同的随机矩阵作为中间结果构造分存图, 方案描述如下.

Wang 等人的 $(2, n)$ 秘密共享方案

输入 黑白图像 A , 参与者个数 $n(n \geq 2)$

输出 分存图 $A_1, \dots, A_n$

分存 步骤 1: 生成 $n+1$ 个随机矩阵 $B_1, \dots, B_n$;

步骤 2: 计算 n 个中间矩阵 $C_1, \dots, C_n$, 其中 $C_i = B_i \wedge A, i = 1, \dots, n$;

步骤 3: 计算 n 个分存图 $A_1, \dots, A_n$, 其中 $A_i = B_{n+1} \oplus C_i, i = 1, \dots, n$.

重构 重构的秘密图像 $A' = A_i \oplus A_j$, 其中 $\{i, j\} \subseteq \{1, \dots, n\}$ 并且 $i \neq j$.

在 Wang 等人的方案中, 对 A 中的任何一个 “0” 像素和任意的 i , 有 $C_i = B_i \wedge 0 = 0, A_i = B_{n+1} \oplus C_i = B_{n+1} \oplus 0 = B_{n+1}$, 于是 $A' = A_i \oplus A_j = B_{n+1} \oplus B_{n+1} = 0$. 而对 A 中的任何一个 “1” 像素和任意的 i , 有 $C_i = B_i \wedge 1 = B_i, A_i = B_{n+1} \oplus C_i = B_{n+1} \oplus B_i$, 于是 $A' = A_i \oplus A_j = B_{n+1} \oplus B_i \oplus B_{n+1} \oplus B_j = B_i \oplus B_j$, 结果可能是 0, 也可能是 1. 换句话说, 在原始秘密图 A 和重构的秘密图 A' 中, A 中的 “0” 像素, 在 A' 中始终被保持不变, 而 A 中的 “1” 像素, 在 A' 中可能是 “1” 像素, 也可能是 “0” 像素. 可以看出 Wang 等人的方案重构复杂度低, 没有像素膨胀, 但是它仅能处理二值图像, 对照度为 $1/2$.

2.2 半色调技术

不同的媒体介质会根据自身的物理特性选用不同的方式来表示图像的色调, 比如, 电脑屏幕使用电流来控制像素的亮度, 而一般的打印机无法直接显示一个图像的灰度级或色调, 只能控制单个像素被打印 (黑色像素) 或不打印 (白色像素). 这种用点的疏密程度来表示不同灰度级的方法, 称为半色调技术. 图 1 显示了连续色调和半色调.

由于半色调图像实际上只有两种颜色: 黑色和白色, 那么针对黑白二值图像的可视分存方案就可以用来构造半色调图像的分存图. Hou^[9] 首先利用半色调技术和图像分解技术, 提出了灰度和彩色图像的可视分存方案. Zhou 等人^[10] 利用半色调技术, 构造了分存图有意义的可视分存方案, 分存图是

图 1 不同灰度级的连续色调和半色调呈现

Figure 1 The continuous tone and halftone for different gray levels

(a) Continuous tone; (b) halftone

半色调图像, 而密图是二值图像. 稍后, 我们所构造的一种灰度图像秘密共享方案, 就用到半色调技术.

3 黑白图像的 $(2, n)$ 秘密共享方案

3.1 r 轮 $(2, n)$ 秘密共享方案的构造

Wang 等人所构造的 $(2, n)$ 秘密共享方案有这样的特点: 原始图像为 “0” 的像素点, 经过分存图的重构, 仍然保持不变, 即条件概率 $p_{0|0} = 1$; 原始图像为 “1” 的像素点, 经过分存图的重构后, 以各自 50% 的概率重构为像素 “0” 或 “1”, 即条件概率 $p_{0|1} = 0.5$ 和 $p_{1|1} = 0.5$. 为了提高重构图像的质量, 需要设法提高条件概率 $p_{1|1}$ 的值. 我们在 Wang 等人的方案的基础上, 进行了一些改进, 引入了布尔或运算 (OR, 记作 “ $\vee$ ”), 提出了针对黑白二值图像的 r 轮 $(2, n)$ 秘密共享方案. 下面用伪代码的形式来描述我们的方案, 包括输入、输出、构造分存图和重构密图等步骤.

黑白图像的 r 轮 $(2, n)$ 秘密共享方案

输入 黑白图像 A , 参与者个数 $n(n \geq 2)$

输出 分存图 $A_{i,1}, A_{i,2}, \dots, A_{i,n}$, 其中 $i = 1, 2, \dots, r, r \geq 1$

分存 for $i = 1$ to r {执行 Wang 等人的 $(2, n)$ 秘密共享方案, 得到 $A_{i,1}, A_{i,2}, \dots, A_{i,n}$;

分发 将分存图 $A_{1,j}, A_{2,j}, \dots, A_{r,j}$ 分发给第 j 个参与者, $j = 1, \dots, n$.

重构 步骤 1: 计算 $T_i = A_{i,j_1} \oplus A_{i,j_2}$, 其中 $i = 1, \dots, r, \{j_1, j_2\} \subseteq \{1, \dots, n\}$ 并且 $j_1 \neq j_2$;
步骤 2: 重构的密图为 $A' = T_1 \vee \dots \vee T_r$.

下面我们给出定理来证明该方案的有效性.

定理 1 用上述算法构造的方案是一个黑白图像的 r 轮 $(2, n)$ 秘密共享方案, 其对照度为 $\alpha^{(r)} = 1 - (1 - \alpha)^r$, 其中 α 是 Wang 等人的 $(2, n)$ -SS 方案的对照度, 即 $\alpha = 1/2$.

证明 首先考虑安全性条件, 所提出的方案是以 Wang 等人的 $(2, n)$ -SS 方案为基础来构建的, 由于 Wang 的方案已证明满足安全性条件, 因此本方案的安全性可以保证.

其次考虑对照度条件, 所提出的方案得到的重构密图是 $A' = T_1 \vee \dots \vee T_r$. 由于各个像素相互独立, 不妨设重构密图中的一个像素为 a , 则 $a = t_1 \vee \dots \vee t_r$, 其中 $t_1, \dots, t_r$ 是各个图 $T_1, \dots, T_r$ 中相应的像素. 只要当 $t_1, \dots, t_r$ 中的某个像素为 “1” 像素, 则像素 a 就为 “1”. 另一方面, 只有当 $t_1 = \dots = t_r = “0”$ 时, 我们才有 $a = “0”$. 由于 $t_1, \dots, t_r$ 是相互独立的, 且具有相同的概率分布, 因此可得到表 1 中 t_i 和 $a = t_1 \vee \dots \vee t_r$ 的概率分布.

由表 1 可知, 新方案的对照度为 $\alpha^{(r)} = 1 - (1 - \alpha)^r$.

在该方案中, r 是一个正整数. 显然, 当 r 变大时, 重构密图的质量会得到显著的提高. 实际上, 当 $r = 1$ 时, 即退化为 Wang 等人的方案.

表 1 t_i 和 $a = t_1 \vee \cdots \vee t_r$ 的概率分布Table 1 Probability distribution for t_i and $a = t_1 \vee \cdots \vee t_r$

Pixel	$p_{0 0}$	$p_{1 0}$	$p_{0 1}$	$p_{1 1}$	$\alpha = p_{1 1} - p_{1 0}$
t_i	1	0	1/2	1/2	1/2
$a = t_1 \vee \cdots \vee t_r$	1	0	$(1 - 1/2)^r$	$1 - (1 - 1/2)^r$	$1 - (1 - 1/2)^r$

图 2 黑白图像的 r 轮 $(2, 3)$ 秘密共享方案的实例Figure 2 An example of r runs $(2, 3)$ -SS scheme for binary image

(a) Secret image; (b) share A_{11} ; (c) share A_{12} ; (d) share A_{13} ; (e) reconstructed secret image of Wang's scheme; (f) reconstructed secret image when $r = 4$; (g) reconstructed secret image when $r = 8$

下面我们将给出一个例子来展示该方案的特点.

例 1 构造 r 轮 $(2, 3)$ -SS 方案, 密图选用 128×128 的黑白 “Lena” 图像. 实验结果如图 2 所示. 图 2(a) 为原始密图, 图 2(b)–(d) 是经过第一轮得到的分存图, 被分发给各个参与者持有, 其他轮所得到的分存图与第一轮类似, 由于篇幅所限, 在此不再展示, 图 2(e) 是用 Wang 等人的 $(2, 3)$ 方案得到的重构结果, 图 2(f)(g) 分别为用 4 轮 $(2, 3)$ -SS 方案和 8 轮 $(2, 3)$ -SS 方案得到的重构结果. 从实验结果可以看出, 每个分存图都与原始密图尺寸相等. 与 Wang 等人的方案相比, 本方案在 r 变大时, 重构密图的质量有了显著的提高.

3.2 与已有方法的比较

表 2 给出了 Yang 的 $(2, n)$ 概率 VSS 方案^[7], Wang 等人的 $(2, n)$ -SS 方案^[11], r 轮 $(2, n)$ -SS 方

表 2 几种不同的 $(2, n)$ 方案所得到的重构密图对照度的比较Table 2 Comparison in terms of the contrast α for different $(2, n)$ schemes

Scheme	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = \infty$
Yang's $(2, n)$ Prob. VSS	1/2	2/7	2/7	1/4	1/5
Wang's $(2, n)$ -SS scheme	1/2	1/2	1/2	1/2	1/2
4 runs $(2, n)$ -SS scheme	15/16	15/16	15/16	15/16	$1 - (1 - 1/2)^4 = 15/16$
8 runs $(2, n)$ -SS scheme	255/256	255/256	255/256	255/256	$1 - (1 - 1/2)^8 = 255/256$
∞ runs $(2, n)$ -SS scheme	1	1	1	1	$1 - (1 - 1/2)^\infty = 1$

案重构密图对照度的比较. 可以看到 r 轮 $(2, n)$ -SS 方案在对照度上优于 Yang 的 $(2, n)$ 概率 VSS 方案和 Wang 等人的 $(2, n)$ -SS 方案, 而且当 r 逐渐变大时, 对照度逐步趋近 1, 即达到近似的精确重构.

3.3 识别区域的讨论

如文献 [7, 11] 所述, 概率秘密共享方案不能保证原始图像中的每一个白色像素 (或黑色像素), 在重构密图中也是白色像素 (或黑色像素), 而是只能通过一块区域反应原始黑白像素的差异. 这样的区域越小, 对应的分存方案也就越好. 我们的方案本质上也是一个概率方案, 因此我们将采用与文献 [11] 类似的分析方法, 来讨论能被正确识别的最小区域, 简称为识别区域.

假定一个区域总共有 N 个像素点, 在这个区域中 “0” 像素点的个数为 S_N . 条件概率 $p_{0|0}$ (或 $p_{0|1}$) 表示原始图像中的 “0” (或 “1”) 像素, 被重构为 “0” 像素的概率. 随机变量 S_N 服从二项分布, 均值和方差分别如下:

$$\begin{aligned}\mu_{0|1} &= N \times p_{0|1}, (\sigma_{0|1})^2 = N \times p_{0|1} \times (1 - p_{0|1}), \\ \mu_{0|0} &= N \times p_{0|0}, (\sigma_{0|0})^2 = N \times p_{0|0} \times (1 - p_{0|0}).\end{aligned}$$

可用正态分布近似逼近二项分布, 依据经验法则, 大约有 99.73% 的值都将落在 $(\mu \pm 3\sigma)$ 区域. 因此, 如果 N 满足如下条件:

$$N > 9 \left(\frac{\sqrt{p_{0|0} \times (1 - p_{0|0})} + \sqrt{p_{0|1} \times (1 - p_{0|1})}}{p_{0|0} - p_{0|1} - d} \right)^2,$$

这个区域将有 99% 的可能性被正确的识别出来, 其中 d 是区分因子, 而且满足 $0 \leq d < p_{0|0} - p_{0|1}$. 在本方案中, $p_{0|0} = 1$, $p_{0|1} = (1 - 0.5)^r$, 因此

$$\begin{aligned}N &> 9 \left(\frac{\sqrt{1 \times (1 - 1)} + \sqrt{(1 - 0.5)^r \times (1 - (1 - 0.5)^r)}}{1 - (1 - 0.5)^r - d} \right)^2 \\ &= 9 \left(\frac{\sqrt{(0.5)^r \times (1 - (0.5)^r)}}{1 - (0.5)^r - d} \right)^2.\end{aligned}$$

表 3 比较了几种方案在不同的区分因子下识别区域的大小. 可以看出, 我们所提出的方案具有非常小的识别区域.

总的来说, 所提出的 r 轮 $(2, n)$ 秘密共享方案比 Wang 等人的 $(2, n)$ 方案具有更高的对照度, 同时保持了低复杂度和没有像素膨胀的优点, 但付出的代价是每个参与者需要持有 r 个分存图.

表 3 几种 $(2, 3)$ -SS 方案在不同的 d 下识别区域的比较Table 3 Comparison of recognition area size for different $(2, 3)$ -SS schemes with different d

d	Ref.[7] $(2, 3)$	Ref.[11] $(2, 3)$	2 runs $(2, 3)$	4 runs $(2, 3)$	8 runs $(2, 3)$
$d = 0.00$	62	9	3	1	1
$d = 0.05$	85	12	4	1	1
$d = 0.10$	126	15	4	1	1
$d = 0.15$	203	19	5	1	1
$d = 0.20$	384	25	6	1	1
$d = 0.30$	6131	57	9	2	1

4 灰度和彩色图像的 $(2, n)$ 秘密共享方案

本节我们将给出两种构造方法 (方法 A 和方法 B) 实现灰度图像的 $(2, n)$ 秘密共享方案. 方法 A 基于半色调技术和布尔运算进行构造, 存储开销较低, 重构密图的质量接近半色调原始密图. 方法 B 基于比特位级别的运算和布尔运算进行构造, 与方法 A 相比有较大的存储开销, 但重构密图的对照度优于方法 A. 在此基础上, 我们将灰度方案扩展到彩色方案.

4.1 方法 A

半色调技术是一种有效的表示灰度图像的方法, 以不同密度的黑白像素点来描述不同的灰度级. 在方法 A 中, 我们首先采用抖动技术将灰度图像 (图 3(a)) 转换成半色调图像, 即黑白二值图像 (图 3(b)), 然后用之前所提出的黑白二值图像的 r 轮 $(2, n)$ 秘密共享方案来进行分存图的构造. 下面用伪代码形式描述方法 A 的输入、输出、分存、分发和重构步骤.

灰度图像的 r 轮 $(2, n)$ 秘密共享方案 — 方法 A

输入 灰度图像 A , 参与者个数 $n(n \geq 2)$

输出 分存图 $A_{i,1}, A_{i,2}, \dots, A_{i,n}$, 其中 $i = 1, 2, \dots, r, r \geq 1$

分存 步骤 1: 将灰度图像 A 转换成半色调图像 HA ;

步骤 2: for $i = 1$ to r {对 HA 执行 Wang 等人的 $(2, n)$ 秘密共享方案, 得到 $A_{i,1}, \dots, A_{i,n}$ };

分发 将分存图 $A_{1,j}, A_{2,j}, \dots, A_{r,j}$ 分发给第 j 个参与者, $j = 1, \dots, n$.

重构 步骤 1: 计算 $T_i = A_{i,j_1} \oplus A_{i,j_2}$, 其中 $i = 1, \dots, r, \{j_1, j_2\} \subseteq \{1, \dots, n\}$ 并且 $j_1 \neq j_2$;

步骤 2: 重构的密图为 $A' = T_1 \vee \dots \vee T_r$.

上述算法构造了适用于灰度图像的 r 轮 $(2, n)$ 秘密共享方案, 重构密图与原始密图大小相同, 且重构密图的质量接近半色调密图, 例 2 给出了采用方法 A 构造灰度图像秘密共享方案的一个实例.

例 2 利用方法 A 构造 r 轮 $(2, 3)$ 秘密共享方案, 原始密图为 256×256 的灰度 “Lena” 图像, 实验结果如图 3 所示. 图 3(a) 表示原始密图, 图 3(b) 表示从原始密图转换得到的半色调密图, 图 3(c)–(e) 是经过第一轮得到的分存图, 图 3(f)–(h) 分别为 r 等于 1、4 和 8 时得到的重构密图. 可以看出每个分存图的尺寸大小与原始图像相同, 当 r 逐渐变大时, 重构密图的质量逐步提升, 当 r 足够大时, 重构密图的质量逼近半色调密图.

图 3 采用方法 A 构造的灰度图像 r 轮 (2, 3) 秘密共享方案的实例

Figure 3 An example of r runs (2, 3)-SS scheme using Method A for grayscale image

(a) Secret image; (b) halftone secret image; (c) share A_{11} ; (d) share A_{12} ; (e) share A_{13} ; (f) reconstructed secret image when $r = 1$; (g) reconstructed secret image when $r = 4$; (h) reconstructed secret image when $r = 8$

4.2 方法 B

灰度图像采用灰度级来描述像素的深浅程度, 通常有 256 个灰度级, 每个灰度级可以用一个 8 比特的二进制向量表示, 因此我们可以将每个灰度级分解成 8 个比特位级, 每一个比特位级构成一幅黑白二值图像. 例如, 考虑如下的灰度图像 $A = \begin{bmatrix} 240 & 118 \\ 50 & 196 \end{bmatrix} = \begin{bmatrix} 11110000 & 01110110 \\ 00110010 & 11000100 \end{bmatrix}$, 我们可将灰度图像 A 分解成 8 个比特位级, 得到 8 个相应的黑白图像, 分别为

$$A^{(1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A^{(2)} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, A^{(3)} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, A^{(4)} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

$$A^{(5)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, A^{(6)} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, A^{(7)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, A^{(8)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

在方法 B 中, 我们首先将一个灰度图像按位分解成 8 个黑白图像, 然后用 3.1 小节中所构造的 r 轮 (2, n) 秘密共享方案对每个黑白图像进行分存图的构建, 最后将对应的 8 个黑白分存图重组为一个灰度分存图. 下面用伪代码形式描述方法 B 的输入、输出、分存、分发和重构步骤.

上述算法构造了适用于灰度图像的 r 轮 (2, n) 秘密共享方案, 重构密图与原始密图大小相同, 且重构密图的质量接近原始密图, 例 3 给出了采用方法 B 构造灰度图像秘密共享方案的一个实例.

灰度图像的 r 轮 $(2, n)$ 秘密共享方案 – 方法 B**输入** 灰度图像 A , 参与者个数 $n(n \geq 2)$ **输出** 分存图 $A_{i,1}, A_{i,2}, \dots, A_{i,n}$, 其中 $i = 1, 2, \dots, r, r \geq 1$ **分存** 步骤 1: 将灰度图像 A 转换分解成 8 个黑白图像 $A^{(1)}, \dots, A^{(8)}$;步骤 2: for $i = 1$ to r { for $k = 1$ to 8{ 对 $A^{(k)}$ 执行 Wang 等的 $(2, n)$ -SS 方案, 得到 $A_{i,1}^{(k)}, \dots, A_{i,n}^{(k)}$; }将 8 个黑白分存图 $A_{i,j}^{(1)}, \dots, A_{i,j}^{(8)}$ 重组为一个灰度分存图 $A_{i,j}$, $j = 1, \dots, n$;

}

分发 将分存图 $A_{1,j}, A_{2,j}, \dots, A_{r,j}$ 分发给第 j 个参与者, $j = 1, \dots, n$.**重构** 步骤 1: 计算 $T_i = A_{i,j_1} \oplus A_{i,j_2}$, 其中 $i = 1, \dots, r, \{j_1, j_2\} \subseteq \{1, \dots, n\}$ 并且 $j_1 \neq j_2$;步骤 2: 重构的密图为 $A' = T_1 \vee \dots \vee T_r$.

例 3 利用方法 B 构造 r 轮 $(2, 3)$ 秘密共享方案, 原始密图为 256×256 的灰度 “Lena” 图像, 实验结果如图 4 所示. 图 4(a) 表示原始密图, 图 4(b)–(d) 是经过第一轮得到的分存图, 图 4(e)–(g) 分别为 r 等于 1、4 和 8 时得到的重构密图. 可以看出每个分存图的尺寸大小与原始图像相同, 当 r 逐渐变大时, 重构密图的质量逐步提升, 当 r 足够大时, 重构密图的质量逼近原始密图.

4.3 方法 A、方法 B 和已有方法的比较

现在, 我们将对采用方法 A 和方法 B 实现的灰度图像 r 轮 $(2, n)$ 秘密共享方案和已有的方案在存储开销和重构密图的对照度两方面进行比较.

- **存储开销** 在 Chang 等人的方案中, 每个参与者持有一个分存图, 分存图的每一个像素占用 8 个比特位. 在方法 A 中, 每一个参与者持有 r 个分存图, 每个分存图都是一幅半色调的黑白图像, 半色调分存图中的每个像素仅占用 1 个比特位, 因此当 $r = 8$ 时, 方法 A 的存储空间与 Chang 等人的方案相等. 方法 B 在比特位级对秘密图像进行分存, 存储开销是 Chang 等人方案的 r 倍, 是方法 A 的 8 倍.

- **对照度** 为了比较重构密图的对照度, 即重构密图与原始密图的接近程度, 我们首先通过一个实验得到主观上的评价, 然后再用峰值信噪比 PSNR(peak signal-to-noise ratio) 进行客观评价.

实验 灰度图像的 $(2, 3)$ 秘密共享方案, 原始密图为 256×256 的灰度 “Lena” 图像. 我们实现了 6 个不同的方案, 分别是

- 1) Wang 等人的方案^[11] (Wang 等人的方案是针对黑白图像构造的, 因此我们首先将灰度图像按位分解成 8 个黑白图像, 然后对每个黑白图像利用 Wang 等人的方案, 再进行重组得到灰度分存图);
- 2) Chang 等人的方案^[13], 参数选择 $b = 4, k = 2, t = 1$;
- 3) 采用方法 A 的 4 轮 $(2, 3)$ 秘密共享方案;
- 4) 采用方法 A 的 8 轮 $(2, 3)$ 秘密共享方案;
- 5) 采用方法 B 的 4 轮 $(2, 3)$ 秘密共享方案;
- 6) 采用方法 B 的 8 轮 $(2, 3)$ 秘密共享方案.

图 4 采用方法 B 构造的灰度图像 r 轮 (2, 3) 秘密共享方案的实例

Figure 4 An example of r runs (2, 3)-SS scheme using Method B for grayscale image

(a) Secret image; (b) share A_{11} ; (c) share A_{12} ; (d) share A_{13} ; (e) reconstructed secret image when $r = 1$; (f) reconstructed secret image when $r = 4$; (g) reconstructed secret image when $r = 8$

图 5 采用不同方案得到的重构密图的比较

Figure 5 The recovered secret image by using different schemes

(a) Wang et al.'s scheme; (b) Chang et al.'s scheme; (c) 4 runs (2, 3)-SS scheme using Method A; (d) 8 runs (2, 3)-SS scheme using Method A; (e) 4 runs (2, 3)-SS scheme using Method B; (f) 8 runs (2, 3)-SS scheme using Method B

表 4 采用不同灰度图像秘密共享方案得到的重构密图的 PSNR 比较

Table 4 Comparison of different grayscale secret sharing schemes with respect to PSNR of the reconstructed image

n	Ref.[11]	Ref.[13]	4 runs (Method B)	8 runs (Method B)
3	25.3441	26.0496	33.0450	45.056962
4	25.3431	26.0228	32.9901	45.1277
10	25.3488	26.0548	32.9999	44.8826

采用上述 6 种方案得到的重构密图如图 5 所示, 可以看出, 我们所提出的方法得到的重构密图的质量要优于 Wang 等人和 Chang 等人的方案, 采用方法 B 得到的重构密图的对照度优于方法 A.

峰值信噪比 (PSNR) 是评价图像质量的一种有效的客观方法, 它的定义式为 $\text{PSNR} = 10 \lg \frac{255^2}{\text{MSE}}$ dB, 其中 MSE 是原始图像和重构图像的均方差. 对一个大小为 $w \times h$ 的原始图像, MSE 的计算公式为 $\text{MSE} = \frac{1}{w \times h} \sum_{i=1}^w \sum_{j=1}^h (I_{i,j} - R_{i,j})^2$, 其中 $I_{i,j}$ 和 $R_{i,j}$ 分别是原始图像和重构图像对应位置的像素值. 表 4 比较了采用方法 B 的 4 轮 $(2, n)$ -SS 方案、8 轮 $(2, n)$ -SS 方案、Wang 等人的方案和 Chang 等人的方案重构密图的 PSNR 值. 方法 A 不在表 4 中, 原因是方法 A 得到的重构密图是半色调图像, 不适合计算 PSNR 值.

从表 4 的 PSNR 这个客观评价标准可以看出, 方法 B 得到的重构密图质量优于 Wang 等人的方案和 Chang 等人的方案.

4.4 彩色图像的 $(2, n)$ 秘密共享方案

下面, 我们将介绍如何将灰度图像的方法 A 和方法 B 扩展到 RGB 彩色图像, 构造彩色图像的 $(2, n)$ 秘密共享方案. 在真彩色模式下, 任何一种颜色都可以由“三原色”, 即红色 (R)、绿色 (G) 和蓝色 (B) 3 种颜色经过一定比例的混合获得. R、G 和 B 三个分量各自用 8 个比特来表示, 可以取 0–255 之间的任何一个数值. 例如, 当用 (R, G, B) 表示一个彩色像素时, (0, 0, 0) 代表全黑, 而 (255, 255, 255) 代表全白.

基于 RGB 彩色图像的特点, 我们可通过 3 个步骤来构造彩色图像的 $(2, n)$ 秘密共享方案. 首先, 将彩色图像分解成 R、G 和 B 3 个分量, 每一分量可以看作一幅灰度图像; 然后, 对每一幅灰度图像 R、G 和 B, 采用灰度图像的方法 A 或方法 B 进行分存图的构造; 最后, 将 3 个分量的分存图进行重组合成, 得到彩色分存图. 彩色图像 r 轮 $(2, n)$ 秘密共享方案的算法描述如下:

彩色图像的 r 轮 $(2, n)$ 秘密共享方案

输入 彩色图像 A , 参与者个数 n ($n \geq 2$)

输出 分存图 $A_{i,1}, A_{i,2}, \dots, A_{i,n}$, 其中 $i = 1, 2, \dots, r, r \geq 1$

分存 步骤 1: 将彩色图像 A 分解成 R、G 和 B 三个分量;

步骤 2: 对每一个 R、G 和 B 分量, 分别执行方法 A (或方法 B), 得到

$$R_{i,1}, R_{i,2}, \dots, R_{i,n}, G_{i,1}, G_{i,2}, \dots, G_{i,n}, B_{i,1}, B_{i,2}, \dots, B_{i,n};$$

步骤 3: 将对应的 $R_{i,j}$, $G_{i,j}$ 和 $B_{i,j}$ 合成为彩色分存图 $A_{i,j}$, 其中 $i = 1, \dots, r, j = 1, \dots, n$.

分发 将分存图 $A_{1,j}, A_{2,j}, \dots, A_{r,j}$ 分发给第 j 个参与者, $j = 1, \dots, n$.

重构 步骤 1: 计算 $T_i = A_{i,j_1} \oplus A_{i,j_2}$, 其中 $i = 1, \dots, r, \{j_1, j_2\} \subseteq \{1, \dots, n\}$ 并且 $j_1 \neq j_2$;

步骤 2: 重构的密图为 $A' = T_1 \vee \dots \vee T_r$.

图 6 采用方法 A 构造的彩色图像 r 轮 (2, 3) 秘密共享方案的实例

Figure 6 An example of r runs (2, 3)-SS scheme using Method A for color image

(a) Secret image; (b) halftone secret image; (c) share A_{11} ; (d) share A_{12} ; (e) share A_{13} ; (f) reconstructed secret image when $r = 1$; (g) reconstructed secret image when $r = 4$; (h) reconstructed secret image when $r = 8$

下面给出两个例子来演示彩色图像 r 轮 (2, n) 秘密共享方案的效果.

例 4 利用方法 A 构造彩色图像的 r 轮 (2, 3) 秘密共享方案, 原始密图为 256×256 的彩色“Lena”图像, 实验结果如图 6 所示. 图 6(a) 表示原始密图, 图 6(b) 表示从原始密图转换得到的半色调密图, 图 6(c)–(e) 是经过第一轮得到的分存图, 其图 6(f)–(h) 分别为 r 等于 1、4 和 8 时得到的重构密图. 可以看出每个分存图的尺寸大小与原始图像相同, 当 r 逐渐变大时, 重构密图的质量逐步提升, 当 r 足够大时, 重构密图的质量逼近半色调密图.

例 5 利用方法 B 构造彩色图像的 r 轮 (2, 3) 秘密共享方案, 原始密图为 256×256 的彩色“Lena”图像, 实验结果如图 7 所示. 图 7(a) 表示原始密图, 图 7(b)–(d) 是经过第一轮得到的分存图, 图 7(e)–(g) 分别为 r 等于 1、4 和 8 时得到的重构密图. 可以看出每个分存图的尺寸大小与原始图像相同, 当 r 逐渐变大时, 重构密图的质量逐步提升, 当 r 足够大时, 重构密图的质量逼近原始密图.

5 总结

本文提出了一种可用于分存黑白、灰度和彩色图像的 r 轮 (2, n) 秘密共享方案. 该方案与传统秘密共享方案相比, 具有较低的计算复杂度; 与可视分存方案相比, 无像素膨胀, 具有更好的对照度; 但其付出的代价是每个参与者需要持有 r 个分存图. 对于黑白图像的 r 轮 (2, n)-SS 方案, 其重构密图

图 7 采用方法 B 构造的彩色图像 r 轮 $(2, 3)$ 秘密共享方案的实例

Figure 6 An example of r runs $(2, 3)$ -SS scheme using Method B for color image

(a) Secret image; (b) share A_{11} ; (c) share A_{12} ; (d) share A_{13} ; (e) reconstructed secret image when $r = 1$;
(f) reconstructed secret image when $r = 4$; (g) reconstructed secret image when $r = 8$

的对照度为 $\alpha^{(r)} = 1 - (1/2)^r$, 当 r 逐渐增大时, 重构密图的质量逐渐变好, r 很大时接近精确重构. 对于灰度和彩色图像, 给出了两种方法构造 $(2, n)$ 秘密共享方案, 得到清晰的重构密图.

参考文献

- 1 Blakley G R. Safeguarding cryptographic keys. Proc Afips Ncc, 1979, 48: 313–317
- 2 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612–613
- 3 Thien C C, Lin J C. Secret image sharing. Comput Graph, 2002, 26: 765–770
- 4 Thien C C, Lin J C. An image-sharing method with user-friendly shadow images. IEEE Trans Circ Syst Vid, 2003, 13: 1161–1169
- 5 Wang R Z, Su C H. Secret image sharing with smaller shadow images. Pattern Recogn, 2006, 27: 551–555
- 6 Naor M, Shamir A. Visual cryptography. In: De Santis A, ed. Advances in Cryptology-EUROCRYPTO'94. Berlin: Springer-Verlag, 1995. 1–12
- 7 Yang C N. New visual secret sharing schemes using probabilistic method. Pattern Recogn, 2004, 25: 481–494
- 8 Cimato S, Prisco R D, Santis A D. Probabilistic visual cryptography schemes. Computer J, 2006, 49: 97–107
- 9 Hou Y C. Visual cryptography for color images. Pattern Recogn, 2003, 36: 1619–1629
- 10 Zhou Z, Gonzalo R A, Crescenzo G D. Halftone visual cryptography. IEEE Trans Image Process, 2006, 15: 2441–2453
- 11 Wang D S, Zhang L, Ma N, et al. Two secret sharing schemes based on Boolean operations. Pattern Recogn, 2007, 40: 2776–2785

- 12 Chao K Y, Lin J C. Secret image sharing: a Boolean-operations-based approach combining benefits of polynomial-based and fast approaches. *Int J Pattern Recogn*, 2009, 23: 263–285
- 13 Chang C C, Lin C C, Le T, et al. A probabilistic visual secret sharing scheme for grayscale images with voting strategy. In: *Proceeding of the International Symposium on Electronic Commerce and Security*. Piscataway: IEEE, 2008. 184–188
- 14 Chang C C, Lin C C, Le T, et al. A new probabilistic visual secret sharing scheme for color images. In: *4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Piscataway: IEEE, 2008. 1305–1308

$(2, n)$ secret sharing scheme based on boolean operation

DONG Lin¹, WANG DaoShun^{1*}, LI ShunDong² & DAI YiQi¹

1 Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

2 School of Computer Science, Shaanxi Normal University, Xi'an 710062, China

*E-mail: daoshun@mail.tsinghua.edu.cn

Abstract Traditional secret sharing (SS) schemes can reconstruct the secret precisely, but have high computation complexity. Visual secret sharing (VSS) schemes use human visual system to reconstruct the secret without cryptographic computation, but have pixel expansion and loss of contrast. Wang et al. proposed a $(2, n)$ -SS scheme for binary images based on Boolean operation, which has low computation complexity, no pixel expansion and the contrast is $1/2$. In this paper, we first construct a r runs $(2, n)$ -SS scheme to improve the contrast of Wang et al.'s binary $(2, n)$ -SS scheme. Then we present two approaches to construct r runs $(2, n)$ -SS schemes for grayscale image and color image. The two approaches are both based on Boolean operation, while one approach uses halftone technology and the other uses bit level processing. These proposed schemes have low computation complexity and almost ideal contrast.

Keywords secret sharing scheme, Boolean operation, halftone, contrast